REMARKS/ARGUMENTS

Amendments

The claims are not modified in the amendment. No claims have been amended, no claims have been cancelled, and no new claims have been added. Therefore, claims 1-2, 4-19 and 21-23 are present for examination. Applicant respectfully requests reconsideration of this application for at least the reasons presented below.

Interview

On February 22, 2005, the Examiner granted an interview to discuss the rejections presented by the Office. No agreement was sought nor was any agreement reached in this just a courtesy call to discuss possible amendments. The Applicant appreciates the granting of this interview and the preparation done beforehand by the examiner.

35 U.S.C. §102 Rejection, Gennaro et al.

The Office Action has rejected claims 1 and 8 under 35 U.S.C. §102(b) as being anticipated by the cited portions of Non-Patent Literature document "How to Sign Digital Streams" of Gennaro et al. (hereinafter "Gennaro"). The Applicant respectfully submits the following arguments pointing out significant differences between claims 1 and 8 submitted by the Applicant and Gennaro.

Claim 1 is directed to "a method for distributing information which includes a signature." This method includes "generating the signature over first information and second information; appending the signature to one of the first information or the second information; sending the first information over a network; sending the second information over the network separately from the step of sending the first information; and sending the signature over the network separately from at least one of the first information or the second information." Claim 8 is directed to "a method for detecting modification of information." The method includes "receiving a signature from the network separately from at least one of the first or second information, wherein the signature is integral to one of the first or second information; and authenticating the signature over the first and second information."

Gennaro is directed to "signing digital streams." (Abstract) Specifically, in the section cited in the Office Action (§1.2, para. 3) Gennaro describes splitting a stream into blocks. (§1.2, para 3, lines 1 and 2) Then, "instead of signing each block, the sender creates a table listing cryptographic hashes of each of the blocks and signs the table." (§1.2, para. 3, lines 2 and 3) "When the receiver asks for the authenticated stream, the sender first sends the signed table followed by the stream." (§1.2, para 3, lines 3 and 4)

That is, the cited portion of Gennaro describes: 1) splitting a stream into blocks; 2) hashing each block and storing the hash value in a table; 3) signing the table; and 4) sending the signed table followed by the stream. It should be noted that the individual blocks are not signed, only the table is signed. In fact, the table of cryptographic hashes is created and signed "instead of signing each block" further indicating that only the table is signed.

The Office Action indicates that "Gennaro discloses generating a signature over first information/hash table and second information/packets." (Para. 7, lines 2 and 3) Since the cited portion of Gennaro does not discuss packets, the Applicant assumes that the Office Action is equating packets to "blocks." The Applicant respectfully disagrees with this reading of Gennaro. Gennaro does not sign packets, blocks, or anything other than the table of hashes. Further, a cryptographic hash as described and used in Gennaro cannot reasonably be considered to be a digital signature. Such a hash can be used to verify the contents of received data, i.e., to verify that the data has not been changed since it was sent, but cannot be used to verify the identity the sender of that data as with a signature. Under Gennaro, the identity of the sender of the signed table can be verified and the contents of the packets can be verified based on the hash values in the table. However, Gennaro does not disclose generating a signature over a first information and a second information and sending the signature over the network separately from at least one of the first information or the second information as recited in claim 1 or receiving a signature from the network separately from at least one of the first or second information, wherein the signature is integral to one of the first or second information and authenticating the signature over the first and second information as recited in claim 8. For at least these reasons, the Applicant requests that the rejection be withdrawn.

35 U.S.C. §102 Rejection, Wong et al.

The Office Action has rejected claims 1 and 8 under 35 U.S.C. §102(e) as being anticipated by the cited portions of Non-Patent Literature document "Digital Signatures for Flows and Multicasts" of Wong et al. (hereinafter "Wong"). The Applicant respectfully submits the following arguments pointing out significant differences between claims 1 and 8 submitted by the Applicant and Wong.

Wong, like Gennaro, is also directed to methods of signing a stream. (Introduction, para. 3) In the cited section (p. 503, col. 1, para. 5 - col. 2, para. 2 and p. 504, col. 1, para. 7 - col. 2, para. 5) two methods are described. The first method begins by computing a message digest for (i.e., hashing) the last packet in the stream. (p. 503, col. 1, para. 5, lines 5-6) This message digest is then concatenated with the next-to-the-last packet for which a message digest is then computed. (p. 503, col. 1, para. 5, lines 6-7) This process of calculating a message digest for a packet, concatenating that message digest to the next prior packet and calculating a message digest for this augmented packet continues backwards through the stream until the first packet is reached. (p. 503, col. 1, para. 5, lines 7-10) Finally, a message digest is calculated for the first, augmented packet in the stream and this message digest, and only this message digest, is signed. (p. 503, col. 1, para. 5, lines 10-11) "In this manner, only one expensive signing/verification operation is needed for the sequence." (p. 503, col. 1, para. 5, lines 11-13)

The other method (i.e., "star chaining") described in the cited portions of Wong describes a block digest that "is simply the message digest of the *m* packet digests (listed sequentially)." (p. 504, col. 1, para. 7, line 2 - col. 2, para. 1, line 1) That is, a message digest is generated for each packet in a block and the list of these message digests is hashed to generate a message digest for the block. (p. 503, col. 2, para. 1, lines 1-4) Finally, this block digest, and only this block digest, is signed to generate the block signature. (p. 503, col. 2, para. 1, lines 4-6)

The methods described in Wong are not unlike those described in Gennaro in that only a single piece of data is signed. In Gennaro, only the table of hash values is signed. In Wong, packets are successively hashed and the resulting single message digest is signed. Wong does not disclose generating a signature over a first information and a second information and sending the signature over the network separately from at least one of the first information or the second information as recited in claim 1 or receiving a signature from the network separately from at least one of the first or second information, wherein the signature is integral to one of the first or second information and authenticating the signature over the first and second information as recited in claim 8. For at least these reasons, the Applicant requests that the rejection be withdrawn.

35 U.S.C. §102 Rejection, Wasilewski'474

The Office Action has rejected claims 1-2, 4-6, 8-9, 11-13 and 21 under 35 U.S.C. §102(e) as being anticipated by the cited portions of U.S. Patent No. 5,870,474 of Wasilewski et al. (hereinafter "Wasilewski '474"). The Applicant respectfully submits the following arguments pointing out significant differences between claims 1-2, 4-6, 8-9, 11-13 and 21 submitted by the Applicant and Wasilewski '474.

As introduced above, claim 1, upon which claims 2 and 4-6 depend, is directed to "a method for distributing information which includes a signature." This method includes "generating the signature over first information and second information; appending the signature to one of the first information or the second information; sending the first information over a network; sending the second information over the network separately from the step of sending the first information; and sending the signature over the network separately from at least one of the first information or the second information."

Also as introduced above, claim 8, upon which claims 9 and 11-13 depend, is directed to "a method for detecting modification of information." The method includes "receiving a signature from the network separately from at least one of the first or second information, wherein the signature is integral to one of the first or second information; and authenticating the signature over the first and second information."

Claim 14, upon which claim 21 depends is directed to "a conditional access system for detecting modification of information." The system includes "authorization information, wherein: a signature is generated over the information object and the authorization information; the information object uses a first transmission pathway to a set top box; the authorization information uses a second transmission pathway to the set top box that is different from the first transmission pathway; the signature uses a third transmission pathway to the set top box that is different from at least one of the first or second transmission pathways; and wherein the signature is integral to one of the information object or the authorization information."

Wasilewski '474 is directed to "a method of providing conditional access to a selected program." (Col. 3, lines 53-54) Under Wasilewski '474 "program bearing packets are encrypted according to a first encryption algorithm using a first key." (Col. 3, lines 56-58) "The first key used to encrypt the program is, in turn, encrypted according to a second encryption algorithm using a second key." (Col. 3, lines 58-60) "The second key is, in turn, encrypted using a public-key cryptographic technique such that the public key used in the encryption corresponds to the private key of the customer's STU." (Col. 3, lines 62-65) In some cases a digital signature may be applied to the encrypted second key. (Col. 4, lines 17-22)

That is, Wasilewski describes a series of successive encryptions in which a first key is used to encrypt a packet, a second key is used to encrypt the first key, and the customer's public key is used to encrypt the second key. Of these keys, Wasilewsi applies a digital signature only to the second key. The encryption of the first key with the multi-session key (MSK) and the encryption of the second key with the user's public key control access to the content but do not affect a signature, only the second key is signed. Therefore, Wasilewski does not disclose generating a signature over a first information and a second information and sending the signature over the network separately from at least one of the first information or the second information as recited in claim 1, or receiving a signature from the network separately from at least one of the first or second information, wherein the signature is integral to one of the first or second information and authenticating the signature over the first and second information as recited in claim 8, or authorization information, wherein: a signature is generated over an information object and the authorization information; the information object uses a first transmission pathway to a set top box; the authorization information uses a second transmission pathway to the set top box that is different from the first transmission pathway; the signature uses a third transmission pathway to the set top box that is different from at least one of the first or second transmission pathways; and wherein the signature is integral to one of the information object or the authorization information as recited in claim 14. For at least these reasons, the Applicant requests that the rejection be withdrawn and claims 1-2, 4-6, 8-9, 11-13 and 21 be allowed.

35 U.S.C. §103 Rejection, Wasilewski '474 in view of Banker et al.

The Office Action has rejected claims 7, 10, 14-15 and 19 under 35 U.S.C. §103(a) as being unpatentable over the cited portions of Wasilewski '474 in view of the cited portions of U.S. Patent No. 5,247,364 of Banker et al. (hereinafter "Banker"). The Applicant respectfully submits that the Office Action does not establish a *prima facie* case of obviousness in rejecting these claims. Therefore, the Applicant requests reconsideration and withdrawal of the rejection.

In order to establish a *prima facie* case of obviousness, the Office Action must establish: 1) some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the references or combine their teachings; 2) a reasonable expectation of success of such a modification or combination; and 3) a teaching or suggestion in the cited prior art of each claimed limitation. See MPEP §706.02(j).

As will be discussed in detail below, the references cited by the Office Action do not teach or suggest each claimed limitation. The Office Action does not provide evidence that the suggestion or motivation to modify or combine the references cited is explicit or implicit in the references cited. Further, the Office Action does not provide any evidence that knowledge of one skilled in the art would provide the suggestion or motivation to modify these references. Finally, the Office Action does not provide evidence of a reasonable expectation of success of such a modification or combination.

As discussed above, independent claim 1, upon which claim 7 depends, claim 8, upon which claim 10 depends, and claim 14, upon which claims 15 and 19 depend, are distinguishable from Wasilewski. Specifically, Wasilewski does not teach or suggest generating a signature over a first information and a second information as recited in claim 1, authenticating the signature over the first and second information as recited in claim 8, or authorization information, wherein a signature is generated over an information object and an authorization information as recited in claim 14.

Banker is directed to "a method and apparatus for tuning channels in a subscription television system having in-band data transmissions." (Col. 1, lines 10-12) Under Banker, an "addressable transmitter transmits data to out-of-band subscriber terminals via a dedicated FM data channel." (Col. 2, lines 55-57) "Scramblers are coupled to headend controller and may be used to selectively scramble television signals for improved security in a subscription television system that is equipped with appropriate descramblers." (Col. 3, lines 47-51) However, Banker does not teach or suggest generating a signature over a first information and a second information and sending the signature over the network separately from at least one of the first information or the second information as recited in claim 1, or receiving a signature from the network separately from at least one of the first or second information, wherein the signature is integral to one of the first or second information and authenticating the signature over the first and second information as recited in claim 8, or authorization information, wherein: a signature is generated over an information object and the authorization information; the information object uses a first transmission pathway to a set top box; the authorization information uses a second transmission pathway to the set top box that is different from the first transmission pathway; the signature uses a third transmission pathway to the set top box that is different from at least one of the first or second transmission pathways; and wherein the signature is integral to one of the information object or the authorization information as recited in claim 14.

The combination of Wasilewski '474 and Banker is no more revelant to the pending claims than either reference alone. Neither Wasilewski '474 nor Banker, alone or in combination, teach or suggest generating a signature over a first information and a second information and sending the signature over the network separately from at least one of the first information or the second information as recited in claim 1, or receiving a signature from the network separately from at least one of the first or second information, wherein the signature is integral to one of the first or second information and authenticating the signature over the first and second information as recited in claim 8, or authorization information, wherein: a signature is generated over an information object and the authorization information; the information object uses a first transmission pathway to a set top box; the authorization information uses a second transmission pathway to the set top box that is different from the first transmission pathway; the signature uses a third transmission pathway to the set top box that is different from at least one of the first or second transmission pathways; and wherein the signature is integral to one of the information object or the authorization information as recited in claim 14. Therefore, the references cited in the Office Action fail to teach or suggest each claimed limitation. Additionally, neither reference suggests such a modification. The Office Action does not provide evidence that the suggestion or motivation to modify or combine the references cited is explicit or implicit in the references cited. Further, the Office Action does not provide any evidence that knowledge of one skilled in the art would provide the suggestion or motivation to modify or combine these references. Finally, the Office Action does not provide evidence of a reasonable expectation of success of such a modification or combination. Therefore claims 7, 10, 14-15 and 19 should be allowed.

35 U.S.C. §103 Rejection, Wasilewski '474 in view of Banker et al. further in view of Shear et al.

The Office Action has rejected claims 16 and 17 under 35 U.S.C. §103(a) as being unpatentable over the cited portions of Wasilewski '474 in view of the cited portions of Banker and further in view of the cited portions of U.S. Patent No. 6,157,721 of Shear et al. (hereinafter "Shear"). The Applicant respectfully submits that the Office Action has not established a *prima facie* case of obviousness in rejecting these claims. Therefore, the Applicant requests reconsideration and withdrawal of the rejection.

As discussed above, independent claim 14 upon which claims 16 and 17 depend is distinguishable from Wasilewski '474 and Banker since neither Wasilewski '474 nor Banker, alone or in combination, teach or suggest authorization information, wherein: a signature is generated over an information object and the authorization information; the information object uses a first transmission pathway to a set top box; the authorization information uses a second transmission pathway to the set top box that is different from the first transmission pathway; the signature uses a third transmission pathway to the set top box that is different from at least one of the first or second transmission pathways; and wherein the signature is integral to one of the information object or the authorization information as recited in claim 14.

Shear is directed to "computer security techniques based at least in part on cryptography, that protect a computer processing environment against potentially harmful computer executables, programs and/or data; and to techniques for certifying load modules such as executable computer programs or fragments thereof as being authorized for use by a protected or secure processing environment." (Col. 1, lines 22-28) Under Shear, "a verifying authority can digitally sign a load module or other executable with several different digital signatures and/or signature schemes." (Col. 7, lines 9-11) That is, "a protected processing environment or other secure execution space may require a load module or other executable to present multiple digital signatures before accepting it." (Col. 7, lines 11-14) In other words, the module may be signed multiple times. However, Shear does not disclose a signature covering more than one module. Therefore, Shear does not teach or suggest authorization information, wherein: a signature is generated over an information object and the authorization information; the information object uses a first transmission pathway to a set top box; the authorization information uses a second transmission pathway to the set top box that is different from the first transmission pathway; the signature uses a third transmission pathway to the set top box that is different from at least one of the first or second transmission pathways; and wherein the signature is integral to one of the information object or the authorization information.

The combination of Wasilewski '474, Banker, and Shear is no more revelant to the pending claims than any of the references alone. None of the references, alone or in combination, teach or suggest authorization information, wherein: a signature is generated over an information object and the authorization information; the information object uses a first transmission pathway to a set top box; the authorization information uses a second transmission pathway to the set top box that is different from the first transmission pathway; the signature uses a third transmission pathway to the set top box that is different from at least one of the first or second transmission pathways; and wherein the signature is integral to one of the information object or the authorization information. Therefore, the references cited in the Office Action fail to teach or suggest each claimed limitation. Additionally, neither reference suggests such a modification. The Office Action does not provide evidence that the suggestion or motivation to modify or combine the references cited is explicit or implicit in the references cited. Further, the Office Action does not provide any evidence that knowledge of one skilled in the art would provide the suggestion or motivation to modify or combine these references. Finally, the Office Action does not provide evidence of a reasonable expectation of success of such a modification or combination. Therefore claims 16 and 17 should be allowed.

35 U.S.C. §103 Rejection, Wasilewski '474 in view of Banker et al. further in view of Wasilewski '866

The Office Action has rejected claim 18 under 35 U.S.C. §103(a) as being unpatentable over the cited portions of Wasilewski '474 in view of the cited portions of Banker and further in view of the cited portions of U.S. Patent No. 5,420,866 of Wasilewski (hereinafter "Wasilewski '866). The Applicant respectfully submits that the Office Action has not established a *prima facie* case of obviousness in rejecting these claims. Therefore, the Applicant requests reconsideration and withdrawal of the rejection.

As discussed above, independent claim 14 upon which claim 18 depends is distinguishable from Wasilewski '474 and Banker since neither Wasilewski '474 nor Banker, alone or in combination, teach or suggest authorization information, wherein: a signature is generated over an information object and the authorization information; the information object uses a first transmission pathway to a set top box; the authorization information uses a second transmission pathway to the set top box that is different from the first transmission pathway; the signature uses a third transmission pathway to the set top box that is different from at least one of the first or second transmission pathways; and wherein the signature is integral to one of the information object or the authorization information.

Wasilewski '866 "is directed to methods for providing conditional access information to decoders in a packet-based multiplexed communications system." (Col. 5, lines 31-33) Wasilewski teaches "methods for providing a plurality of different sets of conditional access information to a remote location and for facilitating access to a selected one of those sets of conditional access information by a decoder at the remote location." (Col. 5, lines 38-43) In other words, Wasilewski teaches encryption of information for controlling access to information but not signatures over that information. Therefore, Wasilewski '866 does not teach or suggest authorization information, wherein: a signature is generated over an information object and the authorization information; the information object uses a first transmission pathway to a set top box; the authorization information uses a second transmission pathway to the set top box that is different from the first transmission pathway; the signature uses a third transmission pathway to the set top box that is different from at least one of the first or second transmission pathways; and wherein the signature is integral to one of the information object or the authorization information.

The combination of Wasilewski '474, Banker, and Wasilewski '866 is no more revelant to the pending claims than any of the references alone. None of the references, alone or in combination, teach or suggest authorization information, wherein: a signature is generated over an information object and the authorization information; the information object uses a first transmission pathway to a set top box; the authorization information uses a second transmission pathway to the set top box that is different from the first transmission pathway; the signature uses a third transmission pathway to the set top box that is different from at least one of the first or second transmission pathways; and wherein the signature is integral to one of the information object or the authorization information. Therefore, the references cited in the Office Action fail to teach or suggest each claimed limitation. Additionally, neither reference suggests such a modification. The Office Action does not provide evidence that the suggestion or motivation to modify or combine the references cited is explicit or implicit in the references cited. Further, the Office Action does not provide any evidence that knowledge of one skilled in the art would provide the suggestion or motivation to modify or combine these references. Finally, the Office Action does not provide evidence of a reasonable expectation of success of such a modification or combination. Therefore claim 18 should be allowed.

35 U.S.C. §103 Rejection, Wasilewski et al. in view of Shear et al.

The Office Action has rejected claims 22 and 23 under 35 U.S.C. §103(a) as being unpatentable over the cited portions of Wasilewski '474 in view of the cited portions of Shear. The Applicant respectfully submits that the Office Action has not established a *prima facie* case of obviousness in rejecting these claims. Therefore, the Applicant requests reconsideration and withdrawal of the rejection.

As discussed above, independent claim 14 upon which claims 22 and 23 depend is distinguishable from Wasilewski '474 and Shear since neither Wasilewski '474 nor Shear, alone or in combination, teach or suggest authorization information, wherein: a signature is generated over an information object and the authorization information; the information object uses a first transmission pathway to a set top box; the authorization information uses a second transmission pathway to the set top box that is different from the first transmission pathway; the signature uses a third transmission pathway to the set top box that is different from at least one of the first or second transmission pathways; and wherein the signature is integral to one of the information object or the authorization information. Therefore, the references cited in the Office Action fail to teach or suggest each claimed limitation. Additionally, neither reference suggests such a modification. The Office Action does not provide evidence that the suggestion or motivation to modify or combine the references cited is explicit or implicit in the references cited. Further, the Office Action does not provide any evidence that knowledge of one skilled in the art would provide the suggestion or motivation to modify or combine these references. Finally, the Office Action does not provide evidence of a reasonable expectation of success of such a modification or combination. Therefore claims 16 and 17 should be allowed.

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance. The issuance of a formal Notice of Allowance at an early date is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 303-571-4000.

Respectfully submitted,

William J. Daley
Reg. No. 52,471

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 303-571-4000 (Denver)
Fax: 303-571-4321 (Denver)
WJD/sbm